Exhibit 5

CSO

SALTED HASH- TOP SECURITY NEWS

By Steve Ragan, Senior Staff Writer, CSO

MAR 8, 2017 8:37 AM PT

About

Fundamental security insight to help you minimize risk and protect your organization

NEWS

SpammerGate: The takeaway lessons and follow-ups on the River City Media data breach

River City Media is ranked in the Top 10 on Spamhaus

On Monday, Salted Hash covered the story of how faulty Rsync backups exposed River City Media (RCM), an organization known to Spamhaus, as its key operators – Alvin Slocombe and Matt Ferris – are listed in the Register of Known Spam Operations (ROKSO).

It's a long story, one that took months to develop with MacKeeper researcher Chris Vickery.

The data breach exposed 1.34 billion email addresses used by RCM to send offers, or emails that most of the public would consider spam. Some of those email records included personal information, compounding the issue. The breach also exposed all of the internals of the company, including intimate details on how they operate.

■ **RELATED: How can you detect a fake ransom letter?**

3	Acme Media
4	Ad Media Plus
5	Bfons, LLC.
6	Blue Fences, LLC.
7	Books Of Wonders For Everyone Inc.
8	Brand 4 Marketing, LLC.
9	Click This, LLC.
10	CloudFly
11	Cloudspace Technologies
12	Cooperative Investments, LLC.
13	DogWorkDot Inc.
14	eBox
15	Fish&Chips
16	ForceNet, LLC.
17	Grow Clientele, LLC.
18	Halofish, LLC.
19	IR Media, LLC.
20	Its Technical, LLC.
21	Jasper Findings, LLC.
22	Jaxer Solutions
23	KN Media, LLC.
24	Klaur Technology
25	Luma Condominiums
26	MIH Marketing, LLC.
27	Media5321, LLC.
28	Micromax Enterprises, LLC.
29	Pheasant Valley Marketing Group
30	RCM Delivery
31	RCM Idaho LLC.
32	River City Media, LLC.
33	Rylekor, LLC.
34	SAMIAM Inc.
35	Site Traffic Network
36	Slip7 Media, LLC.
37	Social Endeavors, LLC.
38	The Wishing Well Company
39	VR Endeavors, LLC.
40	Virtual Ad Group, LLC.
41	WL Web Domains
42	Wharton Dynamics, Inc.
43	Zero Systems, LLC.

Alternate business names used by River City Media

As a result of our story, one of the largest marketing firms working with RCM, Amobee, said the company was dropped from their affiliate service, AdDemand. However, this does nothing to prevent RCM and its staff from switching to a new alias and starting over. In fact, they're already attempting to switch aliases.

Late in the day on Monday, shortly after the story dropped, RCM employees started removing social media profiles and one switched her position from CEO of River City Media, to CEO of Slip7Media. The image to the left is a list of some of the aliases used by RCM, based on insurance documents and domain registrations.

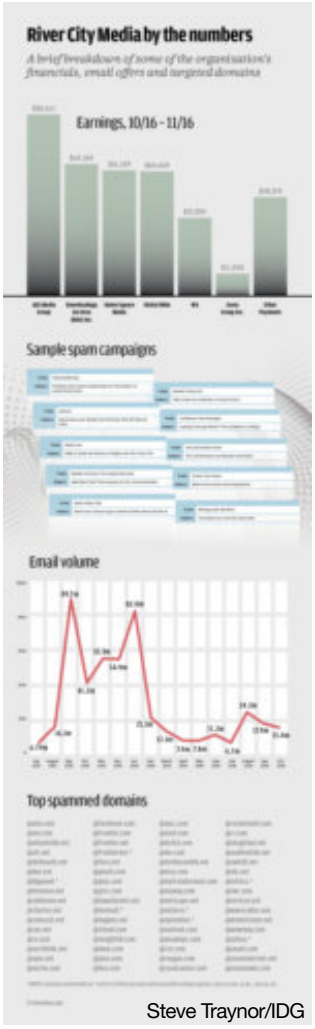
Spamhaus added Domainers Choice (one of the registrars used by RCM) to the number two spot on the Top 10 list of abused domain registrars, the index currently shows that 99.4% of the domains registered there are bad.

The Domainers Choice website is currently offline. Last week, when Salted Hash made attempts to contact them for our story, the website was fully operational. In related news, Salted Hash was pointed to a document from the Internet Corporation for Assigned Names and Numbers (ICANN), which stripped Domainers of accreditation at the beginning of February.

Finally, tests ran on the IP addresses used by RCM and Cyber World Internet Services Inc. show that TierPoint clipped the cord and disconnected the servers sometime on Tuesday. Earlier in the day, the company's MX server was briefly listed by Spamhaus, but that entry was later removed. When asked about the IPs, TierPoint declined to comment and restated their policy to not discuss clients or any client-related issues.

Lessons from the data breach:

While RCM has a bad reputation, and a long history with Spamhaus, they're still a data breach victim. There may be little sympathy for them, but that doesn't alter the facts.



Overview of RCM, including financials and campaigns

RCM had a lot of moving parts, from the thousands of domains and IP addresses, to dozens of providers used to host their infrastructure. Securing one system is hard enough, but securing several of them at scale is a monumental task.

There were so many cooks in the kitchen, a leak like this was always a top risk. Everyone used a cloud-based service of some kind, and everyone was connected to the same back end systems. To top it all off, they were also using personal accounts and systems for work, which only widened their exposure.

While meticulous records helped keep things in order at RCM, those records also helped investigators connect the dots, and helped Spamhaus answer a lot of outstanding questions.

RCM clearly had backup policies and procedures, but it appears they were not fully vetted and tested, because after running smoothly for months, something changed and they were placed on a public-faced server.

Bottom line: The larger the infrastructure, the harder it is to secure

and manage.

Trump Coins:

Commemorative Trum Coin

Early on, one of the River City Media campaigns stood out to us here at Salted Hash, because we were never sure if it was a legitimate offer. In late 2016, after the election in the U.S., the internet was flooded with emails pitching a Trump Coin.

The Trump Coin, at the time, was being pitched as a perfect way to celebrate the President-Elect's victory. But the offer, and the way it was presented, just looked shady. As it turns out, both the offer and the coin were real.

Here are some example ads from the documents exposed by the RCM data breach:

> *From: Donald Trump Coin*
>
> *Subject: THIS Is How You Celebrate A Trump Victory!*
>
> *Subject 2: Trump WINS! And So Do You With THIS Rarity!*

According to AppRiver, the first subject related to the Trump Coin died off on February 14, 2017, and during its lifetime, was observed 271,000 times. The second subject was only seen 79,000 times. AppRiver also observed the following:

> *(69,000 messages) Subject: ALERT: Limited Trump Coin Offer!*
>
> *(88,000 messages) Subject: Boast Your Trump Support With THIS!*

Tools:

Another discovery connected to the RCM data breach are the tools the company used. One set of tools is worth a story on their own, and we'll publish that soon. But there is another set of tools that are worth a mention, because they proved their value when it came to targeting Yahoo and Hotmail.

On January 10 and January 19, 2017, Alvin Slocombe referenced payments made to MyAdTools.com, a company that produces automation tools. The two tools Slocombe mentioned were Yahoo Creator and MailDump Expert. However, the website offers tools for Outlook, AOL GMX, Mail.ru, and Qip.ru creation, as well as tools for Twitter and Skype.

MailDump Expert:

This tool enables the user to extract all of the messages form a given account (Yahoo, AOL, Outlook, Gmail, GMX, etc.), including IMAP/POP3. More than likely, RCM was using this to check where their "offers" were going. It would useful for example, to see if email was hitting a warmup account or seed account. But the exact nature of the tool isn't clear.

Yahoo Creator:

This tool, which works alongside another MyAdTools product (RemoteCaptcha), might explain all of the Yahoo warm-up accounts exposed in the RCM data breach. YahooCreator automates the creation of accounts, and the CAPTCHA work can be outsourced to human CAPTCHA services.

3/8/16: *Updated story to clarify the tools, and link to archived pages. While mentions of them were in the leaked chat logs, their exact use remains unknown, other than how they're referenced on the website where they're ordered.*

Add your lessons learned on our Facebook page.

To comment on this article and other CSO content, visit our Facebook page or our Twitter stream.

Steve Ragan is senior staff writer at CSO. Prior to joining the journalism world in 2005, Steve spent 15 years as a freelance IT contractor focused on infrastructure management and security.

Follow

Healthcare records for sale on Dark Web

You Might Like